Claims

The invention claimed is:

1. A method for calculating the multiplicative inverse of an odd binary number, A, modulo R, where R is a positive integer power of two, 2^k, said method comprising the steps of:

initializing a first storage element having k bits, for a variable S, to a binary 1;

initializing a second storage element having k bits, for a variable Q, with the number A whose multiplicative inverse modulo R is to be determined;

for sequential values of i running from 0 to $k - 1$, carrying out the following operations:

(a) shifting the contents of the first storage element right by one bit position;

(b) determining the current rightmost bit in said first storage element;

(c) upon said rightmost bit position being determined to be a 1, increasing the value stored in said second storage element by 2 and increasing the value stored in said first storage element by A.

2. A method for calculating the negative multiplicative inverse of an odd binary number, A, modulo R, where R is a positive integer power of two, 2^k, said method comprising the steps of:

initializing a first storage element having k bits, for a variable S, to a value of 2^{k-1};

initializing a second storage element having k bits, for a variable Q, with the number A whose negative multiplicative inverse modulo R is to be determined;

for sequential values of i running from 0 to $k - 1$, carrying out the following operations:

(a) shifting the contents of the first storage element right by one bit position;

(b) determining the current rightmost bit in said first storage element;

(c) upon said rightmost bit position being determined to be a 1, decreasing the value stored in said second storage element by 2^i and increasing the value stored in said first storage element by A.

3. A circuit for determining the negative multiplicative inverse of an odd binary number A, modulo R, where R is a positive power of two, 2^k, said circuit comprising:

a first k bit register, for storing a variable S;

a second k bit register, for storing a variable Q;

a third k bit register, for storing said number A;

a counter capable of counting from 0 to $k - 1$;

a decoder receiving count output from said counter;

means for setting bits from said decoder into said first register upon the condition that the next to rightmost bit in said second register is a one;

an adder having as a first input the contents of said second register, and a second input from said third register said second input being conditioned on the next to rightmost bit in said second register, with the output of said adder being supplied to said second register.